Relatório de Incidente de Segurança Cibernética

Seção 1: Identifique o tipo de ataque que pode ter causado esta interrupção da rede

Uma possível explicação para a mensagem de erro de tempo limite na conexão do site é:

Um ataque de negação de serviço (DoS) do tipo **SYN Flood**, que sobrecarrega o servidor com requisições falsas de conexão TCP, impedindo que ele responda aos usuários legítimos.

Os registros mostram que:

O endereço IP **203.0.113.0** enviou um grande número de pacotes **TCP SYN** para o servidor web da empresa (**192.0.2.1**), mas **não completou o handshake TCP**. O servidor responde com SYN-ACKs, aguardando a confirmação (ACK), que nunca chega, o que o leva a manter conexões semiabertas, consumindo recursos.

Este evento pode ser:

Um ataque de **negação de serviço (DoS)** por inundação de pacotes SYN (**SYN Flood**), que esgota os recursos do servidor e afeta a disponibilidade do site.

Seção 2: Explique como o ataque está fazendo o site não funcionar

Quando visitantes do site tentam estabelecer uma conexão com o servidor web, ocorre um aperto de mão triplo usando o protocolo TCP. Explique os três passos do handshake:

1. O cliente envia um pacote **SYN** para iniciar a conexão com o servidor.
2. O servidor responde com um **SYN-ACK**, aceitando a conexão.
3. O cliente finaliza com um **ACK**, confirmando a conexão.

Explique o que acontece quando um agente malicioso envia um grande número de pacotes SYN de uma vez:

O servidor tenta responder com SYN-ACK a cada requisição, mas como o atacante nunca envia o ACK final, o servidor **fica esperando**, mantendo conexões **incompletas**. Quando muitas dessas conexões se acumulam, **o servidor fica sobrecarregado** e não consegue aceitar conexões legítimas.

Explique o que os logs indicam e como isso afeta o servidor:

Os logs mostram uma **repetição intensa de pacotes SYN** vindos do IP **203.0.113.0** em milissegundos de intervalo, com quase nenhuma resposta final (ACK). Isso indica um ataque de **SYN Flood**, que causa **lentidão extrema**, **erros 504 Gateway Timeout**, e até falhas totais no carregamento do site. Visitantes e funcionários não conseguem acessar a página de vendas, afetando a operação da empresa.